IDACS SECURITY

I Introduction

IDACS and its users must conform to State and Federal Laws and rules and regulations handed down by NCIC, NLETS, and the IDACS Committee. All laws and rules are implemented in order to keep the risk to liability low and to insure that the system remains a viable tool.

II. Objective

At the completion of this lesson, the user will be able to answer test questions about rules and regulations, who may access the system, how to handle requests for data, and IDACS Inspections.

III. Finding Rules and Regulations.

1. Indiana Code, IDACS Rules and Regulations

   a. IDACS Manual Part I.
      1. IDACS agreements
         a) Terminal agency agreement
         b) Non-terminal agreements
         c) Statutory police agreement
            1. Indiana Administrative Code
            2. IDACS committee rules/resolutions

   b. IDACS Manual Part II - wanted files criteria for entry and inquiry.

   c. IDACS Manual Part III through VI
      1. BMV data usage rules
      2. NLETS message switching rules
      3. Other misc. file rules

2. NCIC Rules, Federal Law

   a. NCIC Operating Manual
      1. Intro section - system rules
      2. Section 10
         a. III rules.
         b. Federal Title 28.

IV. Who May Access System Data

A. Access, meaning the ability to obtain information from the System, shall be permitted only to criminal justice agencies in the discharge of their official mandated responsibilities, and those agencies as required by state and/or federal enabling authority. Agencies that shall be permitted access to SYSTEM data include the following:

1. Police forces and departments at all governmental levels (including private college and railroad police departments as authorized by Indiana Code) that are responsible for enforcement of general criminal laws.

2. Prosecutive agencies and departments at all governmental levels.

3. Courts at all governmental levels with a criminal or equivalent jurisdiction.

4. Correction departments at all governmental levels, including corrective institutions and probation departments.

5. Parole commissions and agencies at all governmental levels.

6. Agencies at all governmental levels which have as a principle function the collection and provision of fingerprint identification information.

7. Regional or local governmental organizations established pursuant to statute which collect and process criminal justice information and whose policy and governing boards have, as a minimum, a majority composition of members representing criminal justice agencies.

B. Approved noncriminal justice agencies may have access to SYSTEM data on a limited basis. "Limited basis" means restricted to only that data recommended through resolution by the IDACS committee and approved by the state police superintendent.

1. Private Security Agencies and Detectives are not eligible for IDACS information.

C. Verify Authorization Before Releasing Data

1. Require identification.

2. Do not rely on radio as proof.

3. If in doubt, DO NOT RELEASE DATA.

a. Require person to obtain in person.
b. Look up the phone number of the agency and call them back with the reply.
c. Contact IDACS to determine if requesting agency is authorized.

4. By switched message notify SP Data Operations and/or SP IDACS to the attention of IDACS Security of any attempted breaches of security.

V. Enforcement of IDACS Rules, Regulations, Procedures

A. Monitoring System Activity

1. IDACS Transaction Logs - all transactions through the system retained for ten years & periodically reviewed for agency compliance.

2. CHRI Transaction Logs - all CHRI inquiries and responses periodically reviewed for compliance.

3. Quality Control Logs - wanted file activity reviewed daily for errors.

B. Security Inspections and Investigations

1. Security Officers conduct periodic inspections of terminal agencies. Audits shall cover the following areas in connection with both the III and IDACS/NCIC 2000 stolen property and person records:

a. During normal service hours, the operator working is authorized, listed in the certified operator file, and using the correct USERID and Password. All new operators must be fingerprinted and issued an USERID by IDACS, before operating the terminal.

b. If the terminal is secure from public access and view,

1. **240 IAC 5-2-10 Security; confidentiality**…
(1) Security measures for computer centers as follows: (A) All computer sites accessing SYSTEM data shall have the security to protect against any unauthorized access to any of the stored data and/or the computer equipment including the following:
(i) All doors having access to the central processing unit (CPU) room shall be locked at all times.
(ii) A visitor's log shall be maintained of all persons entering the CPU area except those assigned to the area on a permanent basis. The visitor's name, date, time in, time out, agency represented, and reason for visit.

2. (3) Security measures for terminal devices having access to the SYSTEM as follows:
(A) All agencies and computer centers having terminals on the SYSTEM and/or having access to SYSTEM data shall physically place these terminals in a secure location previously approved by the IDACS committee within the authorized agency. Subsequent physical location changes of terminals shall have prior approval of the IDACS committee.

C. Verify proper records are being maintained.

1. CHRI and VGTOF kept for one (1) year.
240 IAC 5-1-3
2. Everything else, including switched messages for (6) months.
240 IAC 5-1-2

D. Testing agencies hit confirmation procedures.

1. Any agency which receives a record(s) in response to an NCIC 2000 inquiry must confirm the hit on any record(s) which appears to have been entered for the person or property inquired upon prior to taking any of the following actions based upon the hit NCIC record:

a. Arresting the wanted person,
b. Detaining the missing person,
c. Seizing the stolen property, or
d. Charging the subject with violating a protection order.

2. Confirming a hit means to contact the agency that entered the record to:

   a. Ensure that the person or property inquired upon is identical to the person or property identified in the record;
   b. Ensure that the warrant, missing person report, protection order, or theft report is still outstanding; and
   c. Obtain a decision regarding:
      1. The extradition of a wanted person when applicable,
      2. Information regarding the return of the missing person to the appropriate authorities,
      3. Information regarding the return of stolen property to its rightful owner, or
      4. Information regarding the terms and conditions of a protection order.

E. Insuring proper documentation is available for each entry in file.

1. **Accuracy** - Any NCIC 2000 entry should contain only correct data. In addition, CTAs should maintain necessary documentation as required by FBI CJIS policy. They should also ensure that documentation is available from state and local users accessing NCIC 2000 through them.

2. **Completeness** - Information contained in an NCIC 2000 entry or in a criminal history record to be disseminated is comprised of all the pertinent available information.

3. **Timeliness** - Entry, modification, update, and removal of information are completed as soon as possible after information is available and information is processed and transmitted in accordance with standards as established by the APB (Advisory Policy Board).

4. **Security** - An organization protects its information against unauthorized access, ensuring confidentiality of the information in accordance with laws and FBI CJIS policy, regulations, and standards.

5. **Dissemination** - All information released is in accordance with applicable laws and regulations, and a record of dissemination of criminal history records is maintained. In addition, CTAs should ensure that documentation is available from local users to assist in biennial state and federal audits.

F. Proper validation procedures are being followed.

1. Validation obliges the ORI to confirm that the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents, and by recent consultation with any appropriate complainant, victim, prosecutor, court, or other appropriate source or individual. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file.

G. Agency and Non-terminal agreements are up-to-date.

1. **240 IAC 5-2-9 User agreement** Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10 Affected: IC 4-1-6-7; IC 10-13-2-6 Sec. 9. All IDACS user agencies shall complete a "user agreement" before utilizing the system. Agencies with terminals and statutory police agencies shall complete such agreements with the Indiana state police and the IDACS committee. Nonterminal agencies shall complete an agreement with the terminal agency that services them. *(State Police Department; Ch I, Sample Agreement; filed Dec 20, 1978, 2:43 p.m.: 2 IR 140; filed Nov 5, 1982, 8:25 a.m.: 5 IR 2490; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2100; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935)*

2. Security Officers investigate:
   a. Violations of law,
   b. Violations of rules, regulations and procedures,
   c. Attempted breaches of security.

3. IDACS Security Officers will report findings to the IDACS Committee for further action.